UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
an iPhone 14 Pro Max, Model MQ8W3LL/A cellular phone, Serial #: MH7W2F9X0J, IMEI 35 739770 063867 8 (See Attachments)

Case No. 22 MJ 185

Matter No.: 2020R00089

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the ______ District of ______
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12/21/2022 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to William E. Duffin.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for ____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of ______.

Date and time issued: 10:38 AM at 12/7/2022

William E. Duffin
Judge's signature

City and state: William E. Duffin

William E. Duffins, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: ________________

Executing officer's signature

Printed name and title

ATTACHMENT A

The property to be searched is as follows ("TARGET CELL PHONE"):

a) an iPhone 14 Pro Max, Model MQ8W3LL/A cellular phone, Serial #: MH7W2F9X0J, IMEI 35 739770 063867 8

The Target Cell Phone is currently located at the U.S. Department of Homeland Security, Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, Suite 600, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the TARGET CELL PHONE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the TARGET CELL PHONE described in Attachment A that relate to violations of Title 18 U.S.C. § 912 (Impersonating an Officer or Employee of the United States) and Title 18 U.S.C. § 1343 (Wire Fraud) since January 2018, including:

    a. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about or associated with impersonating an officer or employee of the United States, as well as fraud by wire, outlined in the affidavit;

2. All names, aliases, and numbers stored in the TARGET CELL PHONE, including numbers associated with the TARGET CELL PHONE.

3. All bank accounts, payment information, transaction records, names, and numbers stored in the TARGET CELL PHONE, including financial accounts associated with the TARGET CELL PHONE, relating to the identities of those involved with the violations.

4. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.

5. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the TARGET CELL PHONE or by other means for the purpose of committing the violations.

6. The list of all telephone calls made or received located in the memory of the TARGET CELL PHONE that provides information regarding the identities of and the methods and means of operation and communication by those engaged in committing the violations.

7. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

8. Evidence of user attribution showing who used or owned the TARGET CELL PHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

9. Any and all information, records, documents, invoices, itineraries, and materials, in any format or medium, pertaining to the travel related to the commission of the violations.

10. Any and all contents of instant messages associated with the TARGET CELL PHONE, including stored or preserved copies of instant messages (including, but not limited to, WhatsApp, iMessages, SMS messages, MMS messages) located on the TARGET CELL PHONE.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

an iPhone 14 Pro Max, Model MQ8W3LL/A cellular phone, Serial #: MH7W2F9X0J, IMEI 35 739770 063867 8 (See Attachments)

Case No. 22 MJ 185

Matter No.: 2020R00089

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the ______________ District of ____________________, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 912	Impersonation of an Officer or Employee of the United States Government
18 U.S.C. § 1343	Fraud by Wire

The application is based on these facts:

See Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ______ days *(give exact ending date if more than 30 days:* __________ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Thomas M. Koch, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 12/7/2022

Judge's signature

City and state: Milwaukee, WI

William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Thomas M. Koch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – one electronic device – which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations (HSI) an investigative branch of the United States Department of Homeland Security (DHS) and have been employed by DHS as a federal law enforcement officer since August 2010. In my employment, I have conducted investigations involving both criminal and administrative violations of federal laws concerning immigration and customs investigations. I have received specialized training from the Federal Law Enforcement Training Centers (FLETC) in Artesia, New Mexico; Charleston, South Carolina; and Glynco, Georgia in the laws and regulations relating to federal criminal and administrative laws, including various types of fraudulent schemes and specifically activities related to immigration and benefit fraud. I have received training and experience in computers and data through various courses in electronic law and evidence, training in seizing computers and other electronic evidence, and other training about the investigative uses of data including how and where it can be located.

3. This affidavit is based upon my personal involvement in this investigation, my training and experience, my review of relevant evidence including victim and witness statements, as well as information supplied to me by other law enforcement officers. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts I believe are necessary to establish probable cause to believe evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 912 (Impersonating an Officer or Employee of the United States) and Title 18 U.S.C. § 1343 (Wire Fraud), incorporated herein by reference as if fully set forth, are located in the TARGET CELL PHONE for which authority is requested to search.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is as follows (herein, "TARGET CELL PHONE"): an iPhone 14 Pro Max, Model MQ8W3LL/A cellular phone, Serial #: MH7W2F9X0J, IMEI 35 739770 063867 8.

6. The TARGET CELL PHONE is currently located at the U.S. Department of Homeland Security, Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, Suite 600, Milwaukee, Wisconsin 53202.

7. The TARGET CELL PHONE was recovered from Juan Carlos MARTINEZ NAPOLES, on October 26, 2022, following his arrest by U.S. Customs and Border Protection Officers at the San Ysidro Port of Entry in San Diego, California when he entered the United States by vehicle from Mexico.

8. The applied-for warrant would authorize the forensic examination of the TARGET CELL PHONE for the purpose of identifying electronically stored data particularly described in Attachment B.

9. The purpose of this application is to seize evidence of violations of violations of Title 18 U.S.C. § 912 (Impersonating an Officer or Employee of the United States) and Title 18 U.S.C. § 1343 (Wire Fraud).

PROBABLE CAUSE

10. On July 27, 2019, Juan Carlos MARTINEZ NAPOLES (MARTINEZ NAPOLES) came to Milwaukee to meet with brothers David Rondin-Rios and Rodrigo Rondin-Rios, David Rondin-Rios's wife (Irma Rondin-Valle), and their nephew (Heisell Rondin-Zendejas). MARTINEZ NAPOLES was previously introduced to the Rondins through another family member in Minnesota who stated MARTINEZ NAPOLES was a U.S. Citizenship and Immigration Services (USCIS) agent and assisted his family in obtaining legal citizenship status. David Rondin-Rios, Rodrigo Rondin-Rios, and Irma Rondin-Valle do not have legal status to enter, remain in, or pass through the United States. Heisell Rondin-Zendejas has been granted Deferred Action for Childhood Arrivals (DACA). Prior to the meeting, David Rondin-Rios, Rodrigo Rondin-Rios, and Irma Rondin-Valle had sent MARTINEZ NAPOLES documents such as their Mexican Birth Certificates, Mexican Consular Cards, and other identification documents. They did this to assist MARTINEZ NAPOLES with his preparation of their immigration paperwork.

11. At this meeting, MARTINEZ NAPOLES stated to the Rondins that he was a federal USCIS agent, and he explained that he worked Monday through Friday doing his job with USCIS and used his personal time to help families expedite the citizenship process. MARTINEZ NAPOLES failed to show any documentation verifying that he was an agent. MARTINEZ NAPOLES provided David Rondin-Rios, Rodrigo Rondin-Rios, and Irma Rondin-Valle envelopes containing partially completed "immigration documents." David Rondin-Rios, Rodrigo Rondin-

Rios, and Irma Rondin-Valle believed that these immigration documents were based on the documents that they had previously sent MARTINEZ NAPOLES. MARTINEZ NAPOLES said that he would pay for immigration form fees, and Heisell Rondin-Zendejas' family could use a payment plan to reimburse him. MARTINEZ NAPOLES said that the form fees for the family would be approximately $14,000 to $15,000.

12. Heisell Rondin-Zendejas informed his family about the July 27 meeting with MARTINEZ NAPOLES, and the opportunity they all had to gain legal immigration status in the United States. Heisell Rondin-Zendejas' father (Gerisel Rondin-Rios), his mother (Clara Zendejas-Pulido), and his sister (Ingrid Rondin-Zejdejas) do not have legal status to enter, remain in, or pass through the United States. On July 29, 2019, Heisell Rondin-Zendejas, Gerisel Rondin-Rios, Clara Zendejas-Pulido, and Ingrid Rondin-Zejdejas texted copies of their identification documents, including Mexican Birth Certificates, Mexican Consular Identification Cards, Mexican Passports, and Wisconsin Identification Cards, to MARTINEZ NAPOLES' cellphone number (385) 272-5556. MARTINEZ NAPOLES then responded via text message confirming receipt of their documents, and he explained he had to wait 72 hours for the system to provide him with their "Alien numbers."

13. On August 10, 2019, MARTINEZ NAPOLES' texted Heisell Rondin-Zendejas from his cell phone number (385) 272-5556 with instructions on how to send him payments. The text messages explained that payments should be sent to the following: Juan Carlos MARTINEZ NAPOLES; JPMorgan Chase Bank Routing Number, 124001545; his Account Number, 521832516; and his email address, 28eolojr@gmail.com. Using this payment information, on August 12, 2019, Clara Zendejas-Pulido sent two payments to MARTINEZ NAPOLES' Chase Bank account with email address 28eolojr@gmail.com, totaling $3,500.

14. On August 20, 2019, MARTINEZ NAPOLES again traveled to Milwaukee to meet with Heisell Rondin-Zendejas, Gerisel Rondin-Rios, Clara Zendejas-Pulido, and the Mercado family, which was also seeking legal immigration status. The Mercado family consisted of Fidel Mercado-Sierra, his wife (Maria Mercado), and their daughter (Gina Mercado). During this meeting, MARTINEZ NAPOLES showed "Social Security Certificates" that he had obtained for David Rondin-Rios, Rodrigo Rondin-Rios, and Irma Rondin-Valle. MARTINEZ NAPOLES also provided Heisell Rondin-Zendejas, Gerisel Rondin-Rios, and Clara Zendejas-Pulido with packets of immigration documents similar to the ones he had provided David Rondin-Rios, Rodrigo Rondin-Rios, and Irma Rondin-Valle during the meeting on July 27. The immigration forms MARTINEZ NAPOLES provided were copies of USCIS Form I-485, Application to Register Permanent Residence or Adjust Status. Copies of these forms were provided to the Milwaukee Police Department (MPD). MARTINEZ NAPOLES informed the group that he had their social security numbers, but the cards had not been printed yet. MARTINEZ NAPOLES also stated to that if they had contact with law enforcement, all they would have to do is provide their Alien number from their forms to the law enforcement officer, and they would be fine. MARTINEZ NAPOLES further explained that he approves immigration applications and also has the power to deport people.

15. Between August 12, 2019 and December 23, 2019, Clara Zendejas-Pulido sent thirteen (13) payments to MARTINEZ NAPOLES' Chase Bank account with email address 28eolojr@gmail.com, totaling $17,055. These payments were for MARTINEZ NAPOLES's travel expenses and costs she was told were related to the legal immigration process.

16. On October 19, 2019, MARTINEZ NAPOLES traveled to Milwaukee, this time meeting with Heisell Rondin-Zendejas, Gerisel Rondin-Rios, Clara Zendejas-Pulido, and Ingrid

Rondin-Zendejas, at a rented space located at 401 W. Michigan Street, Milwaukee. MARTINEZ NAPOLES was in possession of an Apple MacBook laptop and an external Apple trackpad. MARTINEZ NAPOLES explained that he needed to take their fingerprints for their citizenship applications. MARTINEZ NAPOLES then instructed each of the family members individually to place the fingertips of their right hand on the Apple trackpad. When questioned why the "fingerprint scanner" MARTINEZ NAPOLES was using appeared to be a mousepad/trackpad, MARTINEZ NAPOLES became confrontational and threatened, "You guys need somebody that can give you guys more time, so I'm going to transfer your case to someone else, but if whoever that somebody else is sends you a deportation letter, that's out of my hands."

IDENTIFICATION OF MARTINEZ NAPOLES

17. HSI Milwaukee provided MPD a photo of MARTINEZ NAPOLES for use in a photo array. On December 21, 2020, MPD showed victim, Clara Zendejas-Pulido, a photo array consisting of six (6) photographs. Clara Zendejas-Pulido identified the photo HSI Milwaukee provided MPD of MARTINEZ NAPOLES in the photo array as the individual they knew as Juan Carlos MARTINEZ NAPOLES.

DHS EMPLOYMENT STATUS

18. I conducted database searches via internal DHS systems and confirmed MARTINEZ NAPOLES is not an employee of either the Department of Homeland Security or U.S. Citizenship and Immigration Services.

REVIEW OF VICTIM FAMILY IMMIGRATION FORMS

19. I received copies of the USCIS Form I-485s provided to MPD by the victims that were given to them by MARTINEZ NAPOLES. Based on my training and experience, the USCIS Form I-485s MARTINEZ NAPOLES provided appear to be legitimate documents that the public

can access via the USCIS' public website. MARTINEZ NAPOLES filled in the A-File number section on Page 1 of the forms. I conducted searches of DHS databases on all of the A-File numbers MARTINEZ NAPOLES placed on the USCIS Form I-485s and portrayed as legitimate. I was unable to locate any of the A-File numbers in any DHS databases, confirming these A-File numbers are not legitimately assigned to any of the victims. Additionally, the absence of these specific A-File numbers in DHS databases indicate MARTINEZ NAPOLES completely made up these A-File numbers.

20. I conducted a search of the USCIS publicly accessible website. The Form Fee to file the USCIS Form I-485 for a person age 14-78 is currently $1,140 and the Biometric Services Fee is currently $85. The total fee per person to file the USCIS Form I-485 for a person age 14-78 is currently $1,225.

MARTINEZ NAPOLES' CELLPHONE INFORMATION

21. On March 20, 2020, legal process was served on Verizon Wireless requesting information relating to MARTINEZ NAPOLES' account. Requested information received from Verizon Wireless indicates phone number (385) 272-5565 has been associated with account number 473523846-1 since February 13, 2019. Verizon Wireless also indicated this account is registered to MARTINEZ NAPOLES at 3515 W Byde A Wyle, West Valley, Utah 84119.

BANK ACCOUNT INFORMATION

22. On March 20, 2020, legal process was served on JPMorgan Chase Bank requesting financial information related to MARTINEZ NAPOLES' checking account, number 521832516. Requested information received from JPMorgan Chase Bank indicates from August 5, 2019 to the present, checking account number 521832516 has been utilized by MARTINEZ NAPOLES with

a listed address of 3515 S Byde A Wyle, West Valley, Utah 84119 and a telephone number of (385) 272-5556.

23. The following is a list of two deposit transactions received from JPMorgan Chase.

DATE	AMOUNT	TRANSACTION TYPE
8/12/2019	$2,000	Quickpay with Zelle
12/23/2019	$2,000	Quickpay with Zelle

24. These are the specific transactions associated with the victims' payments to MARTINEZ NAPOLES, who said the payments were for fees associated with the immigration process and travel fees.

ARREST OF MARTINEZ NAPOLES, RECOVERY OF TARGET CELL PHONE

25. On October 25, 2022, a federal grand jury in the Western District of Wisconsin indicted Juan Carlos MARTINEZ NAPOLES on two counts of Impersonating an Officer or Employee of the United States in violation of Title 18 U.S.C. § 912, and one count of Fraud by Wire in violation of Title 18 U.S.C. § 1343. Subsequently, an arrest warrant (Case #: 22-cr-211) was issued by the Clerk of Courts in the U.S. District Court for the Eastern District of Wisconsin.

26. On October 26, 2022, MARTINEZ NAPOLES was arrested by U.S. Customs and Border Protection Officers at the San Ysidro Port of Entry in San Diego, California following his arrival to the United States by vehicle from Mexico. At the time of his arrest, MARTINEZ NAPOLES was in possession of the TARGET CELL PHONE. An HSI Special Agent viewed the phone settings of the TARGET CELL PHONE, which indicated MARTINEZ NAPOLES' phone number: (385) 272-5556.

27. Although MARTINEZ NAPOLES' cell phone (TARGET CELL PHONE) was obtained through a lawful search incident to an arrest, in the abundance of caution, your affiant seeks this warrant to search and conduct a forensic examination of the TARGET CELL PHONE.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b) Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c) GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna

receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d) IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

29. Based on my training, experience, and research, and from consulting the manufacturers' advertisements and product technical specifications available online at https://support.apple.com/kb/SP876?locale=en_US, I know the iPhone 14 Pro Max (Model MQ8W3LL/A), cellular telephones have the capability that allow them to serve all or some of the following functions: wireless telephone, a digital camera, GPS navigation device, and accessing /downloading information from the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the TARGET CELL PHONE.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how TARGET CELL PHONE is used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET CELL PHONE because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b) Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the TARGET CELL PHONE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

33. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

34. In conclusion, there is probable cause to believe MARTINEZ NAPOLES' cell phone (TARGET CELL PHONE) will contain information relevant to his illegal activities.

35. I submit this affidavit supports probable cause for a search warrant authorizing the examination of the TARGET CELL PHONE described in Attachment A to seek the items described in Attachment B.

36. Based on the forgoing, I request that the Court issue the proposed search warrant.

ATTACHMENT A

The property to be searched is as follows ("TARGET CELL PHONE"):

a) an iPhone 14 Pro Max, Model MQ8W3LL/A cellular phone, Serial #: MH7W2F9X0J, IMEI 35 739770 063867 8

The Target Cell Phone is currently located at the U.S. Department of Homeland Security, Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, Suite 600, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the TARGET CELL PHONE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the TARGET CELL PHONE described in Attachment A that relate to violations of Title 18 U.S.C. § 912 (Impersonating an Officer or Employee of the United States) and Title 18 U.S.C. § 1343 (Wire Fraud) since January 2018, including:

    a. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about or associated with impersonating an officer or employee of the United States, as well as fraud by wire, outlined in the affidavit;

2. All names, aliases, and numbers stored in the TARGET CELL PHONE, including numbers associated with the TARGET CELL PHONE.

3. All bank accounts, payment information, transaction records, names, and numbers stored in the TARGET CELL PHONE, including financial accounts associated with the TARGET CELL PHONE, relating to the identities of those involved with the violations.

4. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.

5. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the TARGET CELL PHONE or by other means for the purpose of committing the violations.

6. The list of all telephone calls made or received located in the memory of the TARGET CELL PHONE that provides information regarding the identities of and the methods and means of operation and communication by those engaged in committing the violations.

7. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

8. Evidence of user attribution showing who used or owned the TARGET CELL PHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

9. Any and all information, records, documents, invoices, itineraries, and materials, in any format or medium, pertaining to the travel related to the commission of the violations.

10. Any and all contents of instant messages associated with the TARGET CELL PHONE, including stored or preserved copies of instant messages (including, but not limited to, WhatsApp, iMessages, SMS messages, MMS messages) located on the TARGET CELL PHONE.